April 3, 2007

DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION
Enabling Excellence In Delaware State Government

SECURITY - Now ...more than ever!
Cyber Security - Disaster Recovery - Continuity of Government
http://dti.delaware.gov/cybersecurity

eSecurity Advisory

April 3, 2007 MICROSOFT SECURITY BULLETIN RELEASE

The purpose of this update is to provide you with a summary of Microsoft's April 3, 2007 Security Bulletin release. Please note that the security bulletin in this advisory is in addition to what is planned for the normal Microsoft monthly security bulletin release on the 2nd Tuesday of the month.

NEW BULLETINS
Microsoft is releasing the following security bulletins for newly discovered vulnerabilities:

MAXIMUM SEVERITY	BULLETIN NUMBER	PRODUCTS AFFECTED	IMPACT
Critical	MS07-017	Microsoft Windows	Remote Code Execution

A summary for this new bulletin may be found at:
http://www.microsoft.com/technet/security/bulletin/ms07-apr.mspx.

TechNet Webcast:
Information about Microsoft's April Security Bulletin Release
Microsoft will be discussing today's bulletin during their regularly scheduled April 2007 TechNet Security Bulletin webcast. This month, the webcast will be held Wednesday, 11 April 2007 11:00 AM (GMT-08:00) PT. You can register for it here: http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032327017.

Agencies are advised to review the information in the bulletins, test and deploy the updates immediately in their environments, if applicable.

Technical Details

MS07-017

Title: Vulnerabilities in GDI Could Allow Remote Code Execution (925902)

Executive Summary:
This update resolves several newly discovered, publicly disclosed and privately reported vulnerabilities, as well as additional issues discovered through internal investigations. Each vulnerability is documented in its own subsection in the Vulnerability Details section of this bulletin.
An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Note: The Windows Animated Cursor Remote Code Execution Vulnerability - CVE-2007-0038 is currently being exploited and was previously discussed by Microsoft Security Advisory 935423.

Security Update Replacement: This bulletin replaces a prior security update. See the Frequently Asked Questions (FAQ) section of this bulletin (link provided below) for details.

Caveats: Microsoft Knowledge Base Article 925902 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see Microsoft Knowledge Base Article 925902.

Restart Requirement: You must restart your system after you apply this security update.

Removal Information: To remove this update, use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.

Affected Software:

- Windows 2000 Service Pack 4
- Windows XP Service Pack 2
- Windows XP Professional x64 Edition
- Windows XP Professional x64 Edition Service Pack 2
- Windows Server 2003
- Windows Server 2003 Service Pack 1
- Windows Server 2003 Service Pack 2
- Windows Server 2003 for Itanium-based Systems
- Windows Server 2003 with SP1 for Itanium-based Systems
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Server 2003 x64 Edition
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Vista
- Windows Vista x64 Edition

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: **Critical**

More information on this vulnerability is available at:
http://www.microsoft.com/technet/security/bulletin/MS07-017.mspx